Privacy and Security Standards Workgroup
Draft Transcript
March 24, 2011

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good afternoon. This is the Privacy and Security Standards Workgroup call. This is a public call and there will be opportunity at the end for the public to make comments. But first let's do a quick roll call. Dixie Baker.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Walter Suarez.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Anne Castro.

Anne Castro – Blue Cross Blue Shield South Carolina – Chief Design Architect
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Steve Findlay. John Blair. Lisa Gallagher.

Lisa Gallagher – HIMSS – Senior Direct of Privacy & Security
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
David McCallie. Wes Rishel. Sharon Terry.

Sharon Terry – Genetic Alliance – President & CEO
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Steve Ondra. John Halamka. John Moehrke.

John Moehrke – Interoperability & Security, GE – Principal Engineer
John Moehrke is here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Ed Larsen. Mike Davis.

Mike Davis – Veterans Health Administration – Senior Security Architect
Mike Davis is here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Kevin Stine. Adam Greene. Did I miss anyone?

W
John Blair just joined the call.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay, with that I'll turn it over to Dixie Baker.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, and I don't think you've given me control of it. You're going to advance the slides?

Judy Sparrow – Office of the National Coordinator – Executive Director
We can give you control if you would like, Dixie.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I thought you said you were going to do that.

Judy Sparrow – Office of the National Coordinator – Executive Director
Not a problem.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That would be just fine. Thank you. I see it now, thank you very much. Okay, first I want to thank you all for dialing into today's call. It's going to be a very interesting call and I want to start out by introducing to you a new member of our Privacy and Security Workgroup. Lisa Gallagher, who is the Senior Director for Privacy and Security for the Healthcare Information Management System Society, or HIMSS, so, Lisa, we're very, very glad to have you join our workgroup.

Lisa Gallagher – HIMSS – Senior Direct of Privacy & Security
It's good to be here, Dixie. Thank you very much.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Sure. We're basically going to cover two topics today. We're going to briefly go over, not the entire presentation I will present next week, but I did distribute that with the meeting agenda and today's slides and I did receive some comments back and I'll just briefly go over those so that you know the changes that have been made and won't be surprised when they're presented next week. Then the majority of today's call will be on the topic of enterprise level provider directories. We have Hunt Blair from the State of Vermont, HIE; we have Arien Malec talking about the Direct Project. We do not have anyone from Surescripts. We thought we were going to, but we will not. We will have Mike Davis talking briefly about the Veterans Administration's needs in this area and what they're currently doing.

So, with that let me move on to a brief report on the digital certificate work. As I mentioned, I distributed the slides that we intend to use next week. I'm very thankful to Walter, who wisely suggested we move those kinds of tutorial slides back toward the beginning so that we can use them to familiarize the Standards Committee with digital certificates before we launch into the requirements. So, you saw that that was moved back, but still when we deliver the recommendation to the Policy Committee, we will include that tutorial material along with it.

I would say the primary change that I made as a result of some comments that I got from John Moehrke on the digital certificate recommendations was that we don't want to preclude the possibility that we might have a single standard for digital certificates for both Direct exchanges and NwHIN exchanges. Early on we discussed this and we concluded that, well, we probably need two certificates because Direct uses secured e-mail and the NHIN Connect or NHIN Exchange currently uses transport layer security and SOAP Exchanges. So, we proceeded with specifying very minimal, pretty targeted requirements in those two areas, but both John and others, including myself, recognized the value of having a single certificate that's usable for both, if that's possible. So, I've added one bullet at the end of slide nine, I believe it is in that deck, yes, nine; that's the slide that's titled, Recommended Requirements and this additional bullet

says nothing in these requirements precludes the specification of a single standard for a certificate usable for both Direct and NwHIN Exchanges.

Now, does anybody have any objection to that or suggested modification to the working or are you supportive of the idea that we at least leave open the option of having a single standard for both? Anyone?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Dixie, I'm very supportive of that bullet. I think it reads well.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Thank you, thank you, Walter. John, I know that you like opening the door to the possibility and I appreciate, John, all of your comments today. He sent me several— I think that's the primary one. Do you agree, John? I don't think we really need to go over all of the others.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, I agree, Dixie. The other ones were, although critical, were more dressing, if you will. So, yes, that's the important one to hit, I think.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, his other changes really were all excellent ways of making the statement crisper, but this is the one that really has a significant impact on what we're recommending. So, I will copy, well, I'll be sending this on to Judy Sparrow after today's meeting and you'll see it from her for next week's presentation.

So, the plans for the workgroup, report to the Standards Committee. We will be giving them a recommendation. You'll remember that in the slides we recommended that the Policy Committee look into what should be the minimal requirements for an organization that issues digital certificates that could be used for any health exchanges, but in particular those that go over Direct because they aren't under as firm a governance right now as the NwHIN Exchanges are. We recommended that they consider minimum requirements for those certificate authorities that issue certificates. So, that recommendation we will discuss at the Standards Committee and, hopefully, they will agree to send it on.

Today's topic is really focused on entity level provider directories and I will turn this over to Walter. Walter, if you want, I'll just advance the slides. Just say advance and I will.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay, you have control, okay, great. Just to recap a couple of points I think from our previous meeting. We talked with the workgroup about the possibility of basically approaching the discussion on provider directory standards, one we have the recommendations on an individual level provider directories coming from the Policy Committee. So rather than going down the path of starting the discussions on entity level provider directory and then coming to receive the recommendations on the individual level for our directories and doing some more work that might be duplicative in some cases. We requested and we're awaiting the response to move forward with the approach of receiving those recommendations and then working through the two concurrently, the entity level and the individual level.

But in the meantime, as we wait for that, we thought it would be very helpful to bring in this meeting and, perhaps even in the next meeting of the workgroup examples of approaches in the, as we say, in the real world of how organizations—whether it's a state HIE or whether it's a large organization like the VA or other systems—what's our approach for entity level provider directories. That's what we will be discussion and hearing today. At the end, we'll talk about the next meetings of the workgroup after next week's presentation to the Standards Committee, so the meetings we have in April and talk about some of the agenda items that we would look at including in those. So, that's all we were doing.

If we move to our next slide, I think I'm going to just turn it to Hunt to talk about the approach that the State of Vermont is using the experience that they have with this.

Hunt Blair – OVHA – Deputy Director

Thanks, Walter, and thanks, Dixie, and I appreciate the opportunity to talk to the workgroup today. I think it's really appropriate, as you noted in your introduction, Walter, that you're going to look at the ELPD and ILPD together in your discussions going forward because from my point of view and the way that we're approaching this in Vermont, they're very hard to pull apart. I think the process that we went through in the task force to articulate the two was important, but I think as we move into the next phase that the Standards Committee is going to be taking on that it makes sense to be looking at them together.

Just by way of background I wanted to note that our provider directory needs were really generated not just by Health Information Exchange and also not limited to neither just the needs of the Health Information Exchange infrastructure or to support Health Information Exchange, the verb. We have a number of non-HIE use cases where we think that having a robust provider directory is going to be very important for us. Those would include our multi-pair claims database, public health alert systems as well as public health emergency response volunteer systems. And then we have a host of health delivery system reform initiatives that have a substantial amount of tracking and evaluation that is, of course, tied to provider level information and so having a consistent set of authoritative source for which providers are where is incredibly important.

Currently in the state, there just really isn't a place to turn. There are lots of different—I wouldn't think any of them really amount to directories. There are lots of lists in different agencies and departments, but there's not a comprehensive list. There are a lot of inconsistencies in the kinds of information that's found between them so that, for instance, the Board of Medical Practice that licenses physicians as often as not the physicians provide their home address not their place of practice address, so there's a lot of need for multiple reasons for looking at that.

So, as I note in this first slide, we are kind of on this quest for a source of truth. We do have—because we have a functioning exchange—currently there is a provider directory functionally, but one of the things that we've come back to again and again in our discussions with the exchange staff is that they feel a need also to have a more comprehensive authoritative source than just what we have. So, given these different players, obviously, the governance, once we set up the source of truth it's going to be incredibly important for maintaining that and not quickly devolving into differing sources having a different interpretation.

If you want to go to the next slide, so this is really—and I put a little note down at the bottom, this is not a technical picture. This is just a conceptual illustration. I actually showed it to somebody who added a whole bunch more arrows and other boxes and stuff and I said I wouldn't really understand what—I mean, I kind of understood what they were putting on. But my point here is to show that the direction that we're intending to take is that you can see up at the top we're going to have this state provider director, the kind of master directory, the authoritative source, if you will, that will be informed by lots of different sources that are listed to either side there. We'll then use that as both the source for other applications, including as I mentioned before, the multi-pair claims database, our clinical data repository that supports our health reform, delivery system reform and then also to support the Vermont Health Information Exchange Network and its provider directory. Of course, the Health Information Exchange, we have a statewide information exchange. It will be supporting Direct, so it will be important, we just had a meeting this morning, in fact, about the need to get all this up and running so that for Medicare EPs, who are looking to utilize Direct in exchange that we have a place for them to go for determining the routing questions.

So, as I've indicated here it's not clear to us whether the ILPD lives in both places or one, what we're in later slides it shows the level of complexity of interaction that we think we have there. But where I think our current thinking based on our exposure to the discussions through the taskforce and Policy Committee's discussions about ELPDs and ILPDs is that we would anticipate that our state exchange, like probably most state exchanges, would be or have an ELPD, I think, almost extremely likely that it would have at least many ILPD features. There might be more that would be encased in the master directory.

I'm going to go to the next slide.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
One quick question on this slide, is there any particular reason or it's just an artifact of the grants that the arrows are of different sizes?

Hunt Blair – OVHA – Deputy Director
Yeah, I mean I guess this is my kind of funny way of showing that the thought is that the state provider directory, the one up top, is the authoritative source so that it's sort of sending out the truth. But I wanted to also acknowledge that there are going to be sources of information of updates and that sort of thing—so new e-mail address, new fax number, new change of provider's location—that could be coming in from any of the sources. So the thinner lines were meant to indicate that sort of feedback loop and the thicker to indicate that our intent is to have from a governance point of view to have the master directory that the state maintains be sort of at the top of the heap of the governance chain, if you will.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
A lot of providers, individual provider doctors, are also incorporated. Do you then double list them as Dr. Jones person and Dr. Jones, LLC or something?

Hunt Blair – OVHA – Deputy Director
Well, I think that whole question of their roles is a very interesting one and we've had some discussion about that. I should have said at the outset, I kind of alluded to it, but I didn't explain, we are just now in the process of contracting with a consultant. We've been doing a lot of internal work and we got to the point where just because of staff time resources as much as anything we realized that we couldn't carry this forward and get as far as we want. So we've just hired, or are in the process of hiring, a group that's going to help us develop a prototype. I think that a lot of those kind of questions of how we're going to handle roles are going to be sorted out pretty rapidly over the next pretty short timeframe of 12 weeks or 12 to 16 weeks or so.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And you intend for these to include the digital certificates, right?

Hunt Blair – OVHA – Deputy Director
Yeah, so I think that's part of the differentiation between what the exchange, the functionality that they need to have there versus the master director, although I have just demonstrated my own lack of technical understanding of whether or not I've just said something stupid; I mean, maybe we need to have that contained within the master directory also, but certainly the process of doing the certifying would be with the exchange group itself.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Oh, yeah, okay. And that sounds like that's something the consultant will work on.

Hunt Blair – OVHA – Deputy Director
Correct, with our exchange. So the structure in Vermont—I'm the state HIT Coordinator and then we have an external organization called Vital Vermont Information Technology Leaders that operates the exchange, although they, in turn, have a contractor that is the vendor for the exchange. All of us will be getting together to sort through this, hopefully with some clues and insights from the work that your workgroup is going to be doing in the coming weeks.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Just one comment about your question about sole proprietors or incorporated individuals, I remember when the NPI (the National Provider Identifier) system was being developed and we had tons of discussions about that. As many of you know, recall, the NPI separated organizations and individuals by type, so type one were individuals, type two were organizations and when it came to an individual that has "incorporated" the decision was really that if the individual was a sole proprietor, a pure sole

proprietor, as in the IRS regulations define them. That individual would be a type one, an individual and would not be able to obtain a type two entity because the sole proprietor utilizes his or her social security number as the identity for purposes of reporting.

When you have a sole proprietorship or a company that you own as a sole proprietor, when you file taxes you file taxes using a Schedule C and your social security number is the one that is attached to it and so it was decided they were going to be treated as individuals, type one. Now, there's variance about that; a sole proprietor can still go ahead and obtain a tax ID separate from the social security and sort of create the operational implementation of a separate "company." So there were some questions and there are still some issues around that, of course, but generally speaking the individual that acted as a sole proprietor that owns a Dr. Smith Clinic and was a pure sole proprietor was still a type one individual for purposes of the NPI.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's interesting. Thank you.

Hunt Blair – OVHA – Deputy Director
So, should we go on to the next slide? As I said in the beginning, and I think the point about ownership and sole proprietors and the different roles sort of underscores that it's really hard for us to completely separate entities and individuals and so our assumption is that they're going to be extremely interconnected, these two directory functions. I think that the—well, as I said before, we're still determining exactly what the right structure is within the HIE itself, but would mirror at least portions of it.

I think actually if we go to the next slide, and a crazy slide—Walter is familiar with this one because I churned this one out one day during the taskforce call. I think that one of the things, and this, again, is my non-technical perspective on this, but part of what got very confusing in our discussions for me was that we were talking a lot about entity level directories and individual level directories and kind of losing the focus on talking about individuals and entities. I think that the key point of this diagram, such as it is, is just to illustrate that I think any given individual provider is likely to have affiliations with multiple entities and possibly even with multiple locations of a single entity. Walter, I don't know whether you were exaggerating or saying the truth, but you mentioned working at as many as eight different locations. So I think that demonstrates the complexity that we're going to have to have a system that allows for making sure that we're routing data ultimately back to the right place, because I know in Vermont we have physicians who practice at a free clinic, practice at a hospital, maybe practice at a health center one day a week. Obviously, they've got different patients and we want to make sure that the protected health information is getting back to the right place, so, that's, as with many of my drawings, the point is really that there is a lot of confusion there, not that I am proposing the solution exactly.

So, finally, I've already covered what's on the last slide, that we're finalizing our contract for consultants to help us. We're very, I think in a good place in terms of where the discussions are going nationally and our time frame is such that we could really try to develop in the prototype that we're building some modeling of the kinds of approaches that you all will be talking about in the coming weeks.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, thank you. I love this second bullet. I think ONC should put it on a plaque somewhere. That's wonderful. So, thank you very much.

Hunt Blair – OVHA – Deputy Director
Oh, thank you. I look forward to following your deliberations and your recommendations.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, one question, Hunt, again, that relates to where do you see; so, you have a state provider directory, sort of the master directory. You see that being a function of the HIE itself, I presume, and, in fact, it probably is one of those requirements under the HIE cooperative agreement. But is that your expectation that this will be the?

Hunt Blair – OVHA – Deputy Director
Well, I guess it's, I mean, that's if you want to go back to the second slide. What we're imaging—because, sort of going back to the very beginning that we see provider directory use cases that are not just HIE. I mean, for instance, just keeping track of providers data within state government is complicated because we have in the Secretary of State's office the Office or Professional Regulation that keeps track of everybody who is licensed or certified who is not an M.D.

The Department of Public Health has lots of different lists; a lot of the data that is associated with those lists is not necessarily, or is definitely not information that is going to be needed to support the Health Information Exchange, verb or noun. But as long as we're going to the trouble of trying to make sure that we're keeping a current list of all providers and their location and their various roles. Then it seemed like it would be worthwhile to have this broader state function that we have—in Vermont our Division of Healthcare Reform is actually located within the state Medicaid agency. So we have also the additional interest as a Medicaid agency because of our own provider enrollment and listings issues of keeping things clean.

We also, for the EHR incentive program we have an interest in making sure that we have a clean and clear list. So that's why, and to be determined in the weeks and months ahead, our vision at the moment is that there's this kind of loosely coupled architecture between state enterprise system based directory and the directory that the exchange itself, the Health Information Exchange is operating. It could well be that, I mean, I think likely the exchange will just be a mirror of a subset of what's in the main state directory, but that's part of what we're setting out to explore now.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Because what I see in this graph is the right-hand side block where it says VHIE Provider Directory, that seems to me is the provider directory of the Vermont Health Information Exchange, I mean, that's what the name says, right? So, that is, well, that is different from the master state provider directory. That's what I wanted to distinguish.

Hunt Blair – OVHA – Deputy Director
Yeah, I mean it should be highly related, closely related, but yeah, I mean I think that—I mean we've had a series of discussions actually kind of looping back around both about provider directories and actually in master person indexes. One of the things that one of my colleagues keeps pointing out is that the E in EMPI is for Enterprise Master Person Index is the Enterprise and that each, for different reasons each enterprise is going to need its own. So, we kind of have given up on the one server—I know that's probably not exactly the right way to—you know, one database server that's got this directory. Instead, we want to have the different application servers that are in sync with their content.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay, thank you. Any other questions for Hunt?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
We have two more, we have Arien and Mike. Do each of you have time constraints? Does it matter which order or do we just go on to Arien, or what?

Arien Malec – RelayHealth – VP, Product Management
I've got to go off at 3:00.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay, so could you go next?

Arien Malec – RelayHealth – VP, Product Management
I would be happy to. I'm going to apologize and ask you to remind me what I'm supposed to be talking about.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO

This is a session to talk about the entity level provider directories and how the Direct Project is approaching them.

Arien Malec – RelayHealth – VP, Product Management
Excellent. So, thank you very much. There are actually two aspects to entity level provider directories in the Direct Project specifications. The first one is because Direct is built on top of SMTP and S/MIME the first level of this is being able to get the S/MIME package from the sender to the receiver. And this is all very standard Internet-based approach relying on the DNS, so as with any SMTP-based system there are two pre-conditions for exchange to happen.

The first pre-condition is for there to be a DNS named register for the purposes of information exchange. Typically that's going to be something like exchange.sunnyfamilypractice.org or something of the like, or direct.sunnyfamilypractice.org and then that DNS name needs to be registered in the DNS with an MX record that points to it and that lets—one or multiple MX records—and that lets the counterparties for exchange know where to send the package. What happens to the data package after it gets to the destination server is out of scope for Direct. Direct is, as I think many people have noted for Information Exchange, ultimately really at the machine-to-machine exchange level.

The second aspect for which both entity level and individual level directories are necessary, it's for the association between the direct address and the associated certificate. There is an interim way to do this and then there is; actually there are multiple interim ways to do this, but there's at least one interim way to do this and we believe that the long-term answer is in the standards for entity level provider directories that we're talking about.

Direct allows both an organization bound certificate and an individual bound certificate. The organizational bound certificate is only used in a case where the organization can vouch for; there are two preconditions for using the organizational certificate. Precondition number one is that the organization can vouch for and takes responsibility for identity assurance of the addresses associated with that organization. Then number two is that the HIPAA disclosure boundary is at the organizational level. So, a good way to think about using use of organizational certificate is that the organization is really taking responsibility for any disclosure that happens after receiving the data package.

To make Direct work, there needs to be an association between either the organizational certificate or the individual certificate and the Direct address. One way of managing that association is to use a little known, but actually working RFP for storing either the certificate or a pointer to the certificate in the DNS. So there's a mechanism for associating a domain name or an e-mail address with a certificate, actually physically storing the certificate in the DNS or simply point a URL, storing the URL that then points to the certificate. That allows on sending for the sender to retrieve the receiver's certificate for the purposes of encryption. On receipt, of course, based on the SMTP specification the sender certification is actually embedded in the certificate, so you don't need to actually use any further directory structures beyond that.

So, to wrap up, directories for Direct are very simple. The first level of directory is the machine-to-machine directory that's supplied via the DNS. The second level of directory is the association between the Direct address and the associated certificate. There's at least one way of doing that that's also based on the DNS. We believe that the long-term way of doing this is going to be based on the directory approaches that we're all talking about and I believe a requirement for those directories is to have an association between both the organization, the entity and the individual and their associated certificate.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
So, Arien, in terms of these ILPDs and ELPDs, within a Direct context do you see those as two different things? How do you see those?

Arien Malec – RelayHealth – VP, Product Management
Yes, we were talking last call about the thin waste and services on top of the thin waste. From a direct perspective the machine-to-machine directory is absolutely a required for exchange and some ability to look up the certificate is absolutely required for exchange. On top of that there's a set of services that are

useful, but not absolutely required. So, the set of services that are useful are of the nature of I know that Dr. Smith practices in the community, but I don't know Dr. Smith's direct address. Or, I know Dr. Smith practices in the community. I don't know which address it is that I should send a referral document or a CCD. So, discovery both of the entity and the individual as well as discovery of the services that the entity and the individual provides, including the technology services, the content services that are associated are useful, but not essential to exchange. Those, I think, are the key services that will help.

So, the set of essential services that are absolutely required for getting packages from point A to point B and then a set of additional services that, if you will, help lubricate the mechanism of exchange, the gears of exchange to allow for better discovery, better information, etc.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
So, if the thin waste is machine-to-machine exchanges, that's interesting because I think we've talked about entity level provider directories as being more at the organization level, but a machine is not organization level, it's really individual machine address.

Arien Malec – RelayHealth – VP, Product Management
That's right.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, and when you deal with machine-to-machine, yeah, you take out the entire concept of entity and individual at the end of the day.

Arien Malec – RelayHealth – VP, Product Management
At some level you need to map from the entity, the entity Sunny Family Practice to the domain name Sunny Family Practice and then, of course, map from the domain name to the actual physical address where the package gets sent.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Well, one other point is that with the Direct Project it's not exactly machine-to-machine as the end point mail service can have many mail identities there, so we can't really make the exact equivalent of the direct organization-to-organization communication is equivalent to machine-to-machine. It's pretty close, but not identical.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It's really service-to-service, yeah.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
So, taking it, again—well, not to the entity level now, but to the individual level if there are two individuals, literally individuals, like a physician, a doctor sitting at a computer sending a message to another doctor who is in a different organization, sitting at his or her computer. The fact that there are two individuals trying to connect to each other for direct purposes is not necessarily what is important. As I understand it it's really the machine that the doctor is sending the message and the machine that the doctor is receiving it. Is that?

Arien Malec – RelayHealth – VP, Product Management
That's correct and then the associated certificates, yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
And the associated certificates. And the certificates, are the associate certificates certificates related to the entity where the machine lives or are they related to the individual that is using the machine?

Arien Malec – RelayHealth – VP, Product Management
You can do both, or you can do one or the other, I should say. I don't think it would make sense to do both, but you can do one or the other. You can, in the case where the certificate is held at the organizational level, as I said, the pre-conditions for that are that the organization essentially is taking

responsibility for the identity assurance and authentication for any of its endpoints. And is also taking responsibility for disclosure within the organization because the organization is receiving the unencrypted PHI and then is making the appropriate determination of where that unencrypted PHI should go. One additional point for context is that the endpoints, the addresses for exchange don't necessarily correspond to organizations or people. They could also correspond to a referral queue, they could correspond to a lab in box, those kinds of things.

John Moehrke – Interoperability & Security, GE – Principal Engineer
So, Walter, back up to your previous question, they can be specific to the individual, but that creates some disclosure and some medical records tracking issues. So the recommendation at this point from Direct is that you look at this more an organizational communication, but we've also recognized in Direct that to enable specific workflows and automatic measuring and counting you could have the endpoints that you're sending these messages be. Like, Arien says, it could be a lab queue or it could be a departmental queue, so I'm sending this to that department, whoever is in charge today at this particular hour is authorized locally to receive it. So, it's not very tied down as to what the identities are, but once an identity is published by an organization it is published as that identity. It's self-declaring, so to speak.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay, the other question I have is about the certificate discoverability functionality versus the actual certificate. So, I know, Arien, you mentioned that one of the must have essential services is some way to access and basically receive or access or be able to see the certificate information or the certificate of the recipient. The question is really about—and we talked about this at the Policy Committee I remember—whether the directory should include the actual certificate as in like the public key component of the certificate or whether the directory should point to where the certificate is and I suppose it could be either of the two. Because I think, John, you mentioned in some exchange we had why couldn't a certificate, a public key anyway, be available on the directory itself?

John Moehrke – Interoperability & Security, GE – Principal Engineer
I don't think it matters that much, but if I'm going to do one look up, I'd rather do one look up and get the certificate and get redirected to another place to get the certificate. When you're storing things in the DNS it can be more efficient sometimes to use the DNS to just look up the location and then do a secondary look or a secondary pull down from that location. But if I'm already doing, for example, an LDAP-based look up I think my preference would be to do the LDAP look up and actually get the certificate and from a byte perspective, certificates aren't that big. They're DER encoded, even base 64 encoded DER encoded certificates are pretty small objects. It's not like putting a movie into a directory.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
But what happens with respect to maintenance of that information, if the certificate itself is, you know, the issuing entity has sort of the base master information, but then it's also now carried into other places, like this directory and that information changes?

Arien Malec – RelayHealth – VP, Product Management
You've got a very good point there. That's a good motivator for putting a level of interaction.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Well, you update the directory. The certificate is intended to be publicly available. Then yes, you have to know where you have published it or where people expect to find it, and yeah, that thus means that when you do any reissuance or replacement that, yes, you have to update all of those locations where it exists.

Arien Malec – RelayHealth – VP, Product Management
Yes, so I think Walter is really pointing at the issue if he's got replication of directory information, it may be better to store; in some cases, if the replication is slow, it may be better to store the information in one place and just point to it. If the replication is relatively quick, it may not matter that much.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Right, but that would be true of the person's phone number as well.

Arien Malec – RelayHealth – VP, Product Management
Yes.

John Moehrke – Interoperability & Security, GE – Principal Engineer
But, yeah, Walter, there have been cases where the technology chosen to hold a directory could not handle the, it's about 1K or 2K in size of a certificate, depending on if you actually include the full chain. There have been times where the technology chosen can't handle that and that's why they would put in a redirection. The problem I will point out is that if you actually look at the standard for a URL it's about that size as well, so in theory both of them are just about the same size, although URLs usually are practically much smaller than certificates are.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, I wasn't even thinking of the practicality of the size, but more the reality of the accuracy of the information in terms of if it has changed and the directories have not replicated in time then there is some.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, but the result is you will end up with a short-term failure as the receiver of your message will not be able to decrypt the information if it was revoked, but you would then just simply try again, pulling the correct copy of the certificate. The other piece is any time you do a certificate replacement under legitimate purposes you tend to keep both the old and the new for a period of time because of these kinds of issues with certificate distribution being typically slower than normal communication. But that gets into some real operational issues that are way down in the weeds compared to where we should be.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Good point. This is sort of, I mean, a crude comparator or parallel, but it is sort of what happens with the RSA secure ID key that many of us have to enter when logging in securely into our internal systems and all that, you know, the key that is generated every 30 seconds or so. If you enter the key that just is about to expire and then as soon as you hit enter the key expired, the system still keeps sort of the previous key a few more seconds I suppose because you can still log in, right, that kind of a concept.

Arien Malec – RelayHealth – VP, Product Management
It's got grace period built into it, yeah.

John Moehrke – Interoperability & Security, GE – Principal Engineer
They're very different technologies, but that kind of a concept, yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Exactly, no, it's just a crude comparison.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Now the timely piece is far more focused on revocation, which is true of all uses of certificates is revocation tends to be the piece that you have to worry more about timeliness on.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay, any other questions for Arien on the Direct Project? Okay, thanks so much, Arien.

Arien Malec – RelayHealth – VP, Product Management
Thank you very much.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay, we're just in time to let you go. So, I think the last part of the session we were going to ask Mike to talk a little bit about the VA approach and how some of this has been handed in the VA and it was a little different, so, Mike, do you want to talk about that?

Mike Davis – Veterans Health Administration – Senior Security Architect

Sure. I don't have any slides. Can you hear me okay?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, we can hear you okay.

Mike Davis – Veterans Health Administration – Senior Security Architect
Okay, so just a little bit about the VA in this area. First of all, I think just to say upfront that we view the problem in NHIN Exchange and NHIN Direct a little differently and I've made the comment before about keeping NHIN Direct simple. I'm not ready to throw away my fax machine. The fax machines are beautifully efficient and they work really well. It's kind of an amazing thing to see that that infrastructure does work. But it's not an end-squared problem in the fax world like maybe it is in exchange where you have a discovery process and you don't know who you're talking to.

In the fax world, you know who you're talking to. You know people. In San Diego, where I live, the clinicians all know each other, they know their offices and the interaction between different offices and different entities is quite amazing as well as the use of telephones and stuff like that, the point being keep it simple if you could, mantra. Anything that adds complexity is an issue. So, regarding the question here of the enterprise level provider directories, at this point the VA doesn't have any specific approach to this and so we're participating in an NHIN Direct program and in order to be a good partner and to help the development of that kind of an infrastructure. Currently the way the VA has approached it in our pilot demonstrations at HIMSS is what you might expect we do today. An e-mail; there's an initial exchange that's taken place between partners sending e-mails and the credentials are used.

We don't have any directories for this in place, except internally, like Active Directory and that kind of thing, but not for external use. I would say that the VA is a federal agency and so we don't approach this from a proprietary the VA needs to do this point of view, but more from the community of the federal agency's point of view. So we have to comply as a federal agency with what the federal government rules and regulations are. So, we've made this point, I think, many times that we have things like iCam and the Federal Bridge, CH and NIST directives in this area. We have new things like the GSA, Memorandum 11-11; we also have the GSA Trust Framework provider authentication process for Level 1 and 2 certs, we have NISTIR 7497, this is notional architecture for security architecture design process, it's for Health Information Exchange, which recommends Levels 3 and 4.

Then we have iCam, I think I mentioned, the Federal Trust Ecosystem called for in the national strategy for trusted identities in cyberspace. So, the VA, in general, participates in standards organizations. We have a big commitment to that, so our approach is to work within standards organizations and to develop not proprietary, but solutions that work for the community and within the federal government.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Thanks, Mike. Let me test a couple of scenarios and see how this would work in the VA. So, I'm outside of the VA and I'm trying to send a message to a VA clinic in San Diego. So the intent of this entity level provider directory was I would be able to then look up the clinic that I want to send this message entity and find it in the provider directory and then be able to use that information, including the security certificate information to send the message. So, that's one scenario. And the other one—and then I'll let you see how you address how those work in the VA situation—the second one is someone is looking at Dr. Smith, who works in the VA, don't know in which clinic or maybe he works in several clinics. They need to send a message to Dr. Smith in the VA and so trying to find Dr. Smith and trying to find Dr. Smith's location and then the data from a directory that would allow the message to go to Dr. Smith inside the VA is where the applicability of these provider directories will come.

So, how would those two scenarios work in the VA from someone outside trying to send messages?

Mike Davis – Veterans Health Administration – Senior Security Architect
Well, I'm not discounting that provider directory might not be useful, but I'm also just saying that the existing fax system seems to work without a provider directory, so all of those things that you're mentioning seem to be handled today. The VA maintains a Release of Information office, first of all, so a

lot of those kinds of things are not done by individual clinicians; they're handled through the ROI office. So, if a clinician is going to send and direct something to somebody else it's going to go through that ROI office. I think that we shouldn't discount the infrastructure that already exists.

So, if you want to, particularly a small clinic, they don't have a hundred doctors working there, they have a couple or one and the staff knows pretty much everybody. In the community here in San Diego, for example, you know, the clinicians meet together socially, they know each other; it's not like nobody knows anybody. Most of the clinicians know the names of the pharmacists in the pharmacies, they know who they are and they know who to contact if they need to find somebody that they don't know, for example. So, it's just what we do today. People are pretty networked. It's nice to have all automated, and that's great, okay, I'm just saying so what happens if somebody needs to talk to somebody else, they find out who that person is, they would exchange an e-mail to get the credentials and that's it.

If somebody's credentials change they'd probably tell the other party, hey, I've got a new credential, here it is or something like that, but we're not expecting those to change that often, right, anyway. So, I'm just sort of describing them as is situation that we have. When we look at a provider directory those are things that, I guess, have to be maintained. Somebody has to put effort into it to make sure that they information is correct and updated appropriately. But, regardless, we have to have some method of validating that the credentials and the people there are good and they come from a trusted provider, all that kind of stuff.

With respect to the kind of data that might go in there, like I said, the VA doesn't have, that I'm aware of, any specifics other than assurance of the credential itself, but we would work with the community to help define the specifications for such a thing in an interoperable way.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, just to take your example of the facts, we see that it's very reliable, simple and works. There's only one thing that I need to know about that fax machine in order to get the facts there and that is the number. So, I can get the number a couple of ways. Socially I know that there is this group here and maybe I know the fax number. So I already have it memorized and can enter it, or maybe I have my own internal kind of contact list that already has that fax number, my own "provider directory" or directory of external entities I send data to periodically and so it's easy. But there is this situation where I need to send something to a fax machine and I don't have the fax number.

So, of course, I can use the other simple mechanism that we have in place, which is the phone and pick up the phone, call the other place, try to get the fax number, then get the fax number and then enter it and fax whatever I need to send. Or I could have a directory of faxes, if you will, fax machines that can tell me the fax number. And automatically, let's say my fax machine can have some sort of an interface and looks for the fax number of the other entity I'm sending this to and grab it and execute the faxing automatically, I mean that kind of a concept. So that's kind of arguing for the reason behind this need that is being expressed across the board from information exchange entities, whether it's a state HIE, a regional HIE or others for we need a directory where we can find individuals we need to send this information to, or find the entities we need to send this information to.

And it's interesting because you said you already have internally a very sophisticated, very robust provider directory and Kaiser has and pretty much every entity that has multiple providers and multiple locations have those kinds of directories internally to route the information appropriately and all that. And so the question was, yeah, so now we can think of how to make those directories that entities have either operate externally with others so that they can see which locations exist and which providers are part of that and they can route information to those locations or those providers from an external place. I'm just kind of expressing some of the reasons and the purposes for why these provider directories came to be sort of an expectation, a need out there, well, now a requirement as part of the HIE grant to states, basically.

Mike Davis – Veterans Health Administration – Senior Security Architect

Yeah, Walter, I'm not making an argument; let's be clear, I'm not making an argument against directories. That's not what I'm doing. I was asked to talk about what the VA was doing currently and our approach.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
No, I'm not, certainly, arguing or making the statement in response your arguments of somehow not using provider directories. I was just trying to find, basically understand how would you, if there were provider directories out there, how would the VA interact with them, if at all, to route information. You mentioned, for example, that a provider is going to send out something, of course, anything that goes, a disclosure under HIPAA is restricted control and you have an ROI office that handles that. But I'm thinking of incoming traffic.

Mike Davis – Veterans Health Administration – Senior Security Architect
Incoming is handled the same way. The ROI office is the point of contact, so the incoming stuff goes to the ROI office, which returns it to the person that needs it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think Mike's discussion really brings up an interesting point to me is that, you know, I assume that the VA has Active Directory or something like that for your e-mail, right?

Mike Davis – Veterans Health Administration – Senior Security Architect
That's correct, we do, but that's strictly internal.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yeah, but if I wanted to send, I mean we probably all do this all the time, you know, if I wanted to send something to a VA doctor and I knew the domain name, I could probably get it to them, but the point is that there exists already an e-mail level directory in most organizations. So, although that's not called a provider directory, that is certainly a directory that's useful within this context and some questions arise to me is how do those feed into the total scheme of things? How do those regular old e-mail directories that served that purpose fit into the scheme of things?

Mike Davis – Veterans Health Administration – Senior Security Architect
Well, I mean that's a good question, so your question is in the VA, we're talking person-to-person type activities. Like I mentioned, the ROI office, there's two or three people at one of the hospitals at the most who represent that office and so we're not talking about needing to know the addresses of 40,000 or 100,000 people; we need to know a handful, so that's a different level of manageability, right. Again, I'm not arguing against directories.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, I'm just trying to figure out, you know, get the big picture here and I think what you said just brings up those kinds of questions for me.

John Moehrke – Interoperability & Security, GE – Principal Engineer
The other piece of this that I'm hearing, again, this is something I've brought up in other forums is that, and I really like how Mike started this, indicating that really the very nature of the Direct Project does not guarantee that you have an end-squared problem. You really have a small or a manageable list of contacts you are generally going to be communicating with and you're not trying to communicate with any one of the random other people who may have a Direct endpoint.

I think married to that, as Mike is also trying carefully to remind us, if you have a directory you will certainly use it and then the third factor is, once you have communicated a message, a secured message with someone, you know have in your e-mail system the certificate for a return. So, what oftentimes happens in general purpose secure e-mail is one would say, you know, hey, Walter, I would like to send you something secure, could you please send me a signed message.

Walter says, yes, this is the John Moehrke I wanted to communicate with and Walter sends me back a message, here is a signed message. Now, once I have gotten that signed message from Walter, I have

in my e-mail system, it's automatically pulled out of the message and automatically archived in my local, my personal address book, Walter's certificate, and I can return it in a message that is encrypted to Walter. And this conversation didn't require a directory at all. It just simply requires our systems to operate the way that they normally operate when communicating using secured e-mail.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, good point. I mean, absolutely. The only things you would need to know, my address to send me the first message asking, hey, I need to send you something.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, like he said, with a phone number, that's something I can pick up a phone and you say my address is Walter dot, you know, okay, got that. So, you can start this and this is how in social circles it's done; you start it with a social contact. But it's not very formal and that's kind of why people say, well, gee, could we create something more formal, and therefore a directory could be a more formal mechanism to do that. The corollary is once you a directory, you're now publishing e-mail addresses and not only just e-mail addresses that can be harvested for nefarious purposes, but also certificates such that I can now send, as a nefarious person, I can now send you an encrypted message that your normal e-mail spam filters can't protect against.

So, we have to also keep in mind the abuse of a provider directory that includes the certificates, not just how it can enable communication. The social mechanism stops that spam problem, because socially Walter wouldn't respond to someone he didn't want to have a secured conversation with, such as a spammer. Whereas Walter has no control over a spammer using a provider directory to say, oh, Dr. Walter, I want to communicate with him, therefore I will pull his e-mail address out of this provider directory and his certificate and be able to send him encrypted e-mail, which is spam.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's a good point.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
No, excellent point, yeah. The other thing, and this partially was discussed in the several sessions we had with the Policy Committee working on this, the other thing was this example of the e-mail level directory. So, I know there is a Dr. Smith and I know he works for the VA, so if I have the two-part address, the before the at and after the at, I can send to john.smith@va.gov. The message could go through if it is a valid address or it could just be returned because e-mail level directory that the VA has doesn't recognize that entry.

So those were more elements related to kind of the individual. The interesting opportunity about the entity level was knowing that, okay, I'm going to have to send a copy of a CDA report, a hospital discharge summary on a CDA. And I have to send it from the hospital to a clinic and, I mean, all these social mechanisms that allow us to know, yeah, okay, I've done business with this clinic, I have a contract signed and legal people have reviewed it and all that, so I can send that. I know where to send it.

So, that's already established, but it's the ones that are not established that result in I need to send this or who do I send it to? Well, I can pick up the phone, try to figure out that. If I have a fax, I can fax it, you know, on paper. But if I had a provider directory I could pull out the information about the clinic I need to send this or the organization and then be able to delivery that information to the mailbox, perhaps, of that organization that received those types of reports. The organization can then receive it, open it up, find who this is about, in terms of which patient, and find who is the doctor and allocate information into the appropriate medical record, the electronic medical record of that patient. And even send out a message to the doctor saying, hey, we just got a summary report of the hospital of a patient of yours that just came up.

John Moehrke – Interoperability & Security, GE – Principal Engineer
All that process is what provider directory could help support.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
The Policy Committee has decided that we need these provider directories, so I think this discussion needs to get back focused on what information do we need in order to specify the requirements for standards for these directories?

Mike Davis – Veterans Health Administration – Senior Security Architect
I was going to come back and echo some of John's issues with respect to the use of them, and so it may be that the concept of the provider directory isn't necessarily that everybody has access to it. It may be that access for the provider directory could be restricted to people who are authorized to get to that directory and they do that on behalf of their constituents. So, like in the VA it might be the ROI office doing that search on behalf of a clinician and sending the mail to that appropriate person like that rather than everybody having access to it. So, maybe one of our requirements is along the lines of ensuring that access to these directories isn't necessarily available to everyone.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, what you're saying is that the standard itself would need to specify, we need to include the standards for access control for the directory, yeah. Good point, very good point.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
And the Policy Committee also pointed to that fact as well, that the access to, particularly the individual level provider directory would be restricted, it would not be open.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay, that's useful, Mike, thank you.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Well, we have like five more minutes. Thank you, Mike and Hunt and Arien already left, but thanks all for this session. I think it was very valuable to gather all this information about the experiences and the approaches. I'm going to turn it back to Dixie for the last couple of slides, or the last slide, which is the work plan, I think.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, the next steps here is the work plan. So, today is the 24th and the 29th, that's next week, we will be presenting our recommendations to the full Standards Committee on digital certificates, and as you can see in the draft slides we also are just going to give them an update of where we are with respect to provider directories, in general.

So, our next meeting of this workgroup, where we will continue the discussion of provider directories is April the 6th. Now, I did, you'll recall at our last workgroup meeting, at the end I said I would ask for permission from the Standards Committee chairs for us to address ILPDs and ELPDs simultaneously and both of them agreed, both John Perlin and John Halamka agree that that makes a lot of sense, so we'll probably be doing exactly that.

I think John Perlin is waiting for a final yea, verily, that sounds fine from ONC, but I'm confident we will get that, it's just a matter of going through the steps to officially get our charge. The timeline for our charge slightly changed. So, I would expect at our next meeting on April 6th we will be talking about what are some of the standards that we should include in the standards for ELPDs.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Dixie, one suggestion, John brought this up to me. One thought is perhaps to invite the people IT to talk about the IT profile, for example. And the people from HL-7 to talk about the HL-7 standards, kind of the work that is being done around that and that might be something to include on the April 6th call, I think, where we have an hour and a half at least. Because I think, well, for one the recommendation from the Policy Committee on ILPD will not come out until April 13th, which is when the Policy Committee meets to hear the final recommendations and approve them. So they will come after April 13th, so by April 27th, which is our second meeting in April of the workgroup, we will have received those recommendations.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, the ILPD and the ELPD. I think any kind of information that could help us specify the requirements for the standards, without specifying the standards themselves would be useful to us, so, if you want to line that up, Walter, that's perfectly fine with me.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I think in addition, Walter, what may be better is to bring in like the SSA was involved in the IG profile and they had some really interesting insight that they brought to IG and it would be good to have them bring it here rather than have it be desensitized, if you will, through the IG process.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Great, okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Why doesn't Walter work with John, it sounds like he has some experiences behind what went into that profile and decide what would be useful for us to hear at that meeting.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay, will do.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay, are there any other comments? Then why don't we open the line for public comment?

Judy Sparrow – Office of the National Coordinator – Executive Director
Operator, can you check and see if anybody wishes to make a comment?

Operator
You do not have any comments at this time.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay, thank you, Operator. Thank you, Dixie and Walter.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, and thank everyone for dialing in. We appreciate it.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Thank you, bye bye.